UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/306,110	05/06/1999	SATOSHI HASEGAWA	P/2850-19	3039

7590 01/14/2005

Dicksein Shapiro Morin & Oshinsky LLP
1177 Avenue of the Americas
NEW YORK, NY 10036-2714

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 01/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/306,110	HASEGAWA, SATOSHI	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 July 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-9,11 and 14-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-9,11 and 14-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed on July 15, 2005 have been fully considered but they are not persuasive.

It is argued by the applicant that the teachings fail to disclose of an encryption variable that changes at an arbitrary timing and that the timing can be random or regular. Furthermore, it is additionally argued that updated variable is not taught. The examiner disagrees. Wiser is suggestive to modifying the teachings by disclosing that any encryption/decryption method may be used in his system (column 8, lines 50-51). The teachings of Becker are relied upon for the disclosure of to cause random changes in the enciphering keys (column 17, lines 51-56). Becker additionally teaches that these random changes can occur at regular timing based on a clock cycle (column 21, lines 10-16). Since Becker discloses of the usage of changing variables at an arbitrary timing, it is important that the encryption and decryption keys be updated to be synchronized in some manner so that they can be encrypted and decrypted with the correct key.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1,2,5,6,8,9,15, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiser et al in view of Becker.

As per claim 1, Wiser teaches:

calculation means for performing calculation using a variable on an original data stream read from a recording medium so as to produce a calculated data stream (column 2, lines 25-28);

variable creation means for creating the variable (column 4, lines 60-65);

a stream buffer (column 2, lines 24-25);

inverse calculation means for performing inverse calculation on the calculated data stream output from the stream buffer to reproduce the data stream (column 2, lines 29-34;);

stream processing means (column 2, 55-57);

output means (column 2, 31-32).

The teachings of Wiser fail to disclose of using a variable to reproduce the data stream and that the variable is changeable at a regular timing. Wiser does teach that any encryption/decryption method may be used in his system (column 8, lines 50-51). Wiser teaches that encryption/decryption is performed on blocks of data independently. One of ordinary skill would know that frequent key changes strengthen the security of the system.

Becker teaches that one can implement a programmable logic array, PLA,

which is known in the art, to cause random changes in the enciphering keys (column 17, lines 51-56). Becker additionally teaches that these random changes can occur at regular timing based on a clock cycle (column 21, lines 10-16). In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Becker within the system of Wiser because it would allow various keys to encrypt the temporary copy of the data. Wiser teaches that a shortened key is used in this process to make the calculation faster (column 4, lines 63-65), therefore it would have been obvious to one of ordinary skill in the art to change the key frequently to increase the effort needed an outsider to gain knowledge of the entire file.

As per claim 2, Wiser teaches the data streams is read from the recording medium corresponds to an amount of data which can be processed at a time (column 2, lines 20-21).

As per claim 5, Wiser teaches:

calculation means for performing calculation using a variable on an original data stream read from a recording medium so as to produce a calculated data stream (column 2, lines 25-28);

variable creation means; for creating the variable (column 4, lines 60-65);

a stream buffer (column 2, lines 24-25);

inverse calculation means for performing inverse calculation on the calculated data stream output from the stream buffer to reproduce the data stream (column 2, lines 29-34);

stream processing means (column 2, 55-57);

output means (column 2, 31-32)

Wiser is silent in disclosing creating a number of variables. One of ordinary skill would know that using multiple keys and frequently changing them strengthens the security of the system. Becker teaches that one can implement a programmable logic array, PLA, which is known in the art, to cause random changes in the enciphering keys (column 17, lines 51-56). In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Becker within the system of Wiser because it would allow various created keys to encrypt the temporary copy of the data. Wiser teaches that a shortened key is used in this process to make the calculation faster (column 4, lines 63-65), therefore it would have been obvious to one of ordinary skill in the art to change the key frequently to increase the effort needed an outsider to gain knowledge of the entire file.

As per claim 6, Wiser teaches the data streams is read from the recording medium corresponds to an amount of data which can be processed at a time (column 2, lines 20-21).

As per claim 8, Wiser teaches:

calculation means for performing calculation using a variable on an original data stream read from a recording medium so as to produce a calculated data stream (column 2, lines 25-28);

variable creation means for creating the variable (column 4, lines 60-65);

a stream buffer (column 2, lines 24-25);

inverse calculation means for performing inverse calculation on the calculated data stream output from the stream buffer to reproduce the data stream (column 2, lines 29-34);

stream processing means (column 2, 55-57);

output means (column 2, 31-32).

Wiser is silent in disclosing creating a set of variables. One of ordinary skill would know that using multiple keys and frequently changing them strengthens the security of the system. Becker teaches that one can implement a programmable logic array, PLA, which is known in the ad, to cause random changes in the enciphering keys (column 17, lines 51-56). In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Becker within the system of Wiser because it would allow various created keys to encrypt the temporary copy of the data. Wiser teaches that a shortened key is used in this process to make the calculation faster (column 4, lines 63-65), therefore it would have been obvious to one of ordinary skill in the art to change the key frequently to increase the effort needed an outsider to gain knowledge of the entire file.

Wiser is silent in disclosing producing variable change codes representing the variable selected from the variable set. Wiser does teach that any encryption/decryption method may be used in his system (column 8, lines 50-51). Wiser teaches that encryption/decryption is performed on blocks of data independently. Becker teaches that modification modes (variable change codes) result in the changing of keys (variables) (column 2, lines 5.3-59). It is inherent that both the encryption device and decryption device must remain synchronized so that the correct key will be used to decrypt the data. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Becker within the system of Wiser because it is necessary to provide a way in which the decrypting device would know when to use a different key to decrypt data.

As per claim 9, Wiser is silent in disclosing a changing the variable after each cycle. Becker teaches changing the variable after each enciphering operation (cycle) (column 2, lines 53-55). Clearly, the motivation is to increase the overall security of the system. Changing the variable after each cycle greatly increases the work necessary to one trying to compromise the system. The more ways you encipher data, the more ways one has to decipher them. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Becker within the system of Wiser because changing variables after each enciphering cycle to make the system more resistant to unauthorized deciphering.

As per claims 15 and 16, Wiser teaches:

calculation means for performing calculation using a variable on an original data stream read from a recording medium so as to produce a calculated data stream (column 2, lines 25-28);

variable creation means for creating the variable (column 4, lines 60-65);

a stream buffer (column 2, lines 24-25);

inverse calculation means for performing inverse calculation on the calculated data stream output from the stream buffer to reproduce the data stream (column 2, lines 29-34);

stream processing means (column 2, 55-57);

output means (column 2, 31-32).

Wiser is silent in disclosing creating a number of variables. One of ordinary skill would know that using multiple keys and frequently changing them strengthens the security of the system. Becker teaches that one can implement a programmable logic array, PLA, which is known in the art, to cause random changes in the enciphering keys (column 17, lines 51-56). In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Becker within the system of Wiser because it would allow various created keys to encrypt the temporary copy of the data. Wiser teaches that a shortened key is used in this process to make the calculation faster (column 4, lines 63-65), therefore it would have been obvious to one of ordinary skill in the art to change the key frequently to increase the effort needed an outsider to gain knowledge of the entire file.

Wiser is silent in disclosing producing variable change codes periodically. Wiser does teach that any encryption/decryption method may be used in his system (column 8, lines 50-51). Wiser teaches that encryption/decryption is performed on blocks of data independently. Becker teaches that modification modes (variable change codes) result in the changing of keys (variables) (column 2, lines 53-59). It is inherent that both the encryption device and decryption device must remain synchronized so that the correct key will be used to decrypt the data. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Becker within the system of Wiser because it is necessary to provide a way in which the decrypting device would know when to use a different key to decrypt data.

Wiser is silent in disclosing of changing the variable after each cycle. Becker teaches changing (update) the variable after each enciphering operation (cycle or timing) (column 2, lines 53-55). Clearly, the motivation is to increase the overall security of the system. Changing the variable after each cycle greatly increases the work necessary to one trying to compromise the system. The more ways you encipher data, the more ways one has to decipher them. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Becker within the system of Wiser because changing variables after each enciphering cycle to make the system more resistant to unauthorized deciphering.

4. Claims 4,7,11, and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiser et al in view of Becker, in further view of Mionet et al.

As per claims 4, 7, 11, and 14, the examiner supplies the same rationale as recited in the rejection of claim 1 for the motivation to include the teachings of Becker within the system of Wiser. Wiser and Becker are silent in disclosing a message representing a variable change code. Mionet teaches that in order for the decrypting device to know when to use a new key, that the encryption device sends a message to the decrypting device indicating when a new key is to be used (column 9, line 65-column 10, lines 15). Mionet uses a message to indicate a key change instead of just sending the new key over the transmission means. If one were to send the new key encrypted with the old key and the old key had been comprised then they new key would also be compromised. It is inherently insecure to send a key in the clear. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to pass a variable change code from the calculator to the inverse calculator because it is more secure than sending the new key encrypted by the old key. In the context of Wise, it is obvious that the code must travel from the calculator to the inverse calculator via the buffer because that is the only data path to connecting the two.

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CR

January 10, 2004